UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/730,167 | 12/05/2003 | Thomas A. Crispin | CNTR.2224-C1 | 2865 |

23669 7590 06/04/2008

HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

| EXAMINER | |
|---|---|
| GYORFI, THOMAS A | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 06/04/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/730,167 | CRISPIN ET AL. | |
| | Examiner | Art Unit | |
| | Thomas Gyorfi | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *10 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-22,24,25,27,56-64,66-76 and 79-83* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22,24,25,27,56-64,66-76 and 79-83* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/21/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-22, 24, 25, 27, 56-64, 66-76, and 79-83 remain for examination. The correspondence filed 3/10/08 amended claims 1, 13, 24, 25, 56, 79, 81, & 82; and cancelled claims 23, 26, 77, & 78.

### *Continued Examination Under 37 CFR 1.114*

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/10/08 has been entered.

### *Information Disclosure Statement*

3. The information disclosure statement (IDS) submitted on 11/21/07 which had not been considered in the previous Office Action, has now been considered by the Examiner.

### *Response to Arguments*

4. It is observed that both the Applicant and the Examiner have supplied conflicting references in an attempt to establish what exactly is meant by the claim term “microprocessor”.[1] However, based upon the disclosure found within the instant specification itself wherein the term "microprocessor" is

[1] Examiner notes that the Wikipedia article cited by the Applicant was published circa 2008, and can hardly be relied upon as prior art. Examiner has included earlier revisions of pertinent Wikipedia articles that would qualify as prior art, or at least significantly predate the Applicant's references, herein.

contextually defined in a manner so as to exclude co-processors (see paragraph 0017 on pages 11-12; cf. the amendment of 3/10/08, page 24, 2nd paragraph), Applicant's arguments filed 3/10/08 are thus found to be persuasive. Accordingly, the rejections of at least claims 1 and 56 based under 35 USC 102(e), as well as those other rejections predicated on the rejections of claims 1 and 56, are withdrawn. However, new grounds of rejections are presented herein in view of the newly discovered reference to Best.

5. Examiner also wishes to note for the record that Examiner disagrees with Applicant's argument on page 25 of the amendment, where "Applicant also asserts that the cryptographic operation is performed *atomically* responsive to a *cryptographic instruction*, as opposed to a plurality of primitives, which is taught by Kessler." Assuming this argument is applicable only to claim 1, it is noted that the claim language does not in fact make a distinction of any kind as to whether the cryptographic instruction may or may not be comprised of a series of primitives. However, as it is unclear from the context whether this argument could also be applied to independent claim 56, Applicant is cautioned that doing so would incur a rejection under 35 USC 112, 2nd paragraph, as that conflicts with the claim language which explicitly recites "translation logic" precisely for the purpose of implementing a cryptographic instruction as a series of primitives, just as found in the Kessler reference.

## ***Claim Rejections - 35 USC § 103***

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1-6, 11, 12, 24, 25, 27, 56-60, 66, and 79-83 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al. (U.S. Patent 6,789,147) in view of Best (U.S. Patent 4,278,837).

Regarding claims 1 and 56:

Kessler discloses a microprocessor apparatus for performing a cryptographic operation, the appartus comprising: fetch logic, configured to fetch an instruction flow from memory for execution by a microprocessor (col. 4, line 59 – col. 5, line 36), said instruction flow comprising an instruction, configured to direct said microprocessor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 – col. 6, line 10); and a cryptography unit, disposed within execution logic in said microprocessor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55); and an integer unit, disposed within execution logic in said microprocessor and coupled in parallel with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operation (col. 9, lines 15-20).

The microprocessor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred narrow definition of "microprocessor" established in the specification. However, Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, either preferably as the sole processor in a computing apparatus, or alternatively by creating a hybrid wherein a conventional microprocessor and the cryptographic coprocessor are combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col. 19, lines 20-60; Figures 17 & 18). The claims are thus obvious because the technique of physically incorporating a cryptographic co-processor, such as that disclosed by Kessler, into a conventional microprocessor to create a hybrid microprocessor to be used as the CPU for a computing apparatus had clearly been long since known as being well within the ordinary capabilities of one skilled in the art.

Regarding claim 56:

Kessler discloses an apparatus for performing cryptographic operations, comprising: fetch logic, disposed within a microprocessor, configured to fetch an instruction flow from memory for execution by a microprocessor by said microprocessor (col. 4, line 59 – col. 5, line 36), said instruction flow comprising an instruction, configured to direct said microprocessor to perform the cryptographic operation (col. 4, lines 10-16; col. 5, lines 29-36; Figure 7), wherein said cryptographic instruction prescribes one of the cryptographic operations (Figure 3); said cryptographic operation comprising: an opcode field, configured to prescribe that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory (element 302 of Fig. 3; col. 5, lines 37-50); and a repeat prefix field, coupled to said opcode field, configured to indicate that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a

plurality of blocks of input data (element 310 of Fig.3; col. 5, line 50 – col. 6, line 10); translation logic, disposed within said microprocessor, configured to translate said cryptographic instructions into associated micro instructions that specify sub operations required to accomplish said one of the cryptographic operation (e.g. col. 8, lines 11-16); and a cryptography unit, disposed within execution logic in said microprocessor, configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by said control word (col. 9, lines 7-55).

The microprocessor disclosed by Kessler is a coprocessor, which by itself does not conform to Applicant's preferred narrow definition of "microprocessor" established in the specification. However, Best discloses wherein microprocessors with dedicated cryptographic functionality could be employed in an apparatus, either preferably as the sole processor in a computing apparatus, or alternatively by creating a hybrid wherein a conventional microprocessor and the cryptographic coprocessor are combined into one single, indivisible microprocessor that behaves in exactly the manner as the "microprocessor" of the instant application (col. 19, lines 20-60; Figures 17 & 18). The claims are thus obvious because the technique of physically incorporating a cryptographic co-processor, such as that disclosed by Kessler, into a conventional microprocessor to create a hybrid microprocessor to be used as the CPU for a computing apparatus had clearly been long since known as being well within the ordinary capabilities of one skilled in the art.

Regarding claims 2 and 83:

Kessler further discloses wherein the cryptographic operations are accomplished at the level of system privileges afforded to application programs (SSL being a component of web browser applications: col. 4, lines 5-10).

Regarding claims 3 and 57:

Kessler further discloses an encryption operation encrypting a plurality of blocks of input data to generate a plurality of ciphertext blocks (e.g. col. 2, lines 13-14 etc.)

Regarding claims 4 and 58:

Kessler further discloses an decryption operation decrypting a plurality of blocks of input data to generate a plurality of plaintext blocks (Ibid).

Regarding claims 5 and 59:

Kessler further discloses using AES (col. 9, lines 13-15; element 807 of Figure 8).

Regarding claims 6 and 60:

Kessler further discloses a block cipher mode to be employed in accomplishing the cryptographic operations (inherent to the block ciphers taught in col. 9, lines 10-20).

Regarding claim 11:

Kessler further discloses wherein the instruction proscribes that the cryptographic operations be accomplished on a plurality of text blocks (Figure 7)

Regarding claims 12 and 66:

Examiner takes Official Notice that the "prior art microprocessor" component of the hybrid microprocessor disclosed by Best would be an x86 processor, with instructions prescribed in the x86 instruction format (see the enclosed “X86 architecture” Wikipedia reference, subsection "History", regarding the obviousness of the above).

Regarding claims 24 and 79:

Kessler further discloses block cipher logic, configured to perform a plurality of cryptographic rounds on each of said plurality of blocks of input data according to said one of the block

cryptographic operations to produce said corresponding plurality of output text blocks (col. 9, lines 7-44); and key RAM, operatively coupled to said block cipher logic, configured to store a key schedule, said key schedule comprising a plurality of round keys, each corresponding to a plurality of cryptographic rounds, and configured to provide each of said plurality of round keys to said block cipher logic for performance of said each of said plurality of cryptographic rounds (col. 9, lines 23-55).

Regarding claims 25 and 80:

Kessler further discloses wherein said block cipher logic id divided into two or more stages, whereby said plurality of cryptographic rounds are simultaneously performed on two or more of said plurality of blocks of data (inherent to at least the AES and 3DES algorithms disclosed on col. 9, lines 10-20).

Regarding claims 27 and 82:

Kessler further discloses wherein said opcode field directs said cryptography unit to load one of said each of said plurality of input text blocks and to perform said plurality of cryptographic rounds (col. 5, lines 40-50).

Regarding claim 81:

Kessler further discloses an integer unit, coupled in parallel with said cryptography unit, configured to execute a plurality of integer operations that are required to accomplish the cryptographic operations (arithmetic unit: col. 9, lines 15-20).

8. Claims 7-10 and 61-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler in view of Best as applied to claims 6 and 60 above, and further in view of the "Applied Cryptography, 2nd Edition" (hereinafter, "Schneier"; submitted by Applicant in the IDS forms filed 9/25/05 and 3/11/06).

Regarding claims 7-10 and 61-64:

Although Kessler and Best both disclose using block cipher modes for at least some of the supported encryption algorithms, they do not explicitly mention any of the modes listed in these claims. However, Schneier teaches that each mode (ECB, CBC, CFB, and OFB) were well known in the art (pages 193-206); accordingly, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use any of these modes in the cryptographic processor disclosed by Kessler [as modified by Best]; each mode has its own particular advantages as disclosed by Schneier (page 209, as appropriate).

9. Claims 13-22 and 67-76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler as applied to claims 1 and 56 above, and further in view of Johns-Vano et al. (U.S. Patent 6,026,490)

Regarding claims 13 and 67:

Although Kessler and Best both disclose at least one register (Kessler: element 220 of Figure 2; Best: col. 5, lines 35-50 and Figures 8 & 9), it is unclear as to whether the instruction implicitly references a plurality of registers in the device. However, Johns-Vano discloses that the instruction set of a cryptographic processor implicitly references a plurality of internal registers (elements 558, 560, 564, 552, 566, and 556 of Figure 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made for a cryptographic processor to employ a plurality of registers. One would do so because using hardware registers would be conducive to making a cryptographic processing engine suitable for manufacture in semiconductor foundries thereby reducing manufacturing costs (col. 2, lines 28-33).

Regarding claims 14 and 68:

Johns-Vano further discloses a first register, wherein contents of said first register comprise a pointer to a first memory address, said first memory address specifying a first location in said memory for access of a plurality of input text blocks upon which the cryptographic operations is to be accomplished (col. 5, lines 1-55).

Regarding claims 15 and 69:

Johns-Vano further discloses a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing the cryptographic operations upon a plurality of input text blocks (col. 5, lines 1-55).

Regarding claims 16 and 70:

Johns-Vano further discloses a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks (col. 5, lines 1-55).

Regarding claims 17 and 71:

Johns-Vano further discloses a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in said memory for access to cryptographic key data for use in accomplishing the cryptographic operations (col. 5, lines 1-55).

Regarding claims 18 and 72:

Kessler and Johns-Vano further disclose wherein said cryptographic key data comprises a cryptographic key (Kessler: col. 6, lines 40-50; Johns-Vano: col. 7: 1-5).

Regarding claims 19 and 73:

Kessler further discloses wherein said cryptographic key data comprises a cryptographic key schedule (inherent to the algorithms used in col. 9, lines 10-20).

Regarding claims 20 and 74:

Johns-Vano further discloses a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in said memory for access of an initialization vector for use in accomplishing the cryptographic operations (col. 5, lines 1-55).

Regarding claims 21 and 75:

Johns-Vano further discloses a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in said memory for access of said control word for use in accomplishing the cryptographic operations, wherein said control word prescribes cryptographic parameters for cryptographic operations (col. 5, lines 1-55).

Regarding claims 22 and 76:

Kessler further discloses an encryption/decryption field, configured to prescribe whether the cryptographic operation is an encryption operation or a decryption operation (col. 5, lines 50-60).

## ***Conclusion***

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: various Wikipedia articles from 2003 that further support the idea that a CPU [a "microprocessor" in the parlance of the specification] could be comprised of coprocessors, and furthermore wherein some Intel X86 processors (such as the 386DX) included math coprocessors

whereas others (such as the 386SX) lacked them, thus requiring external coprocessors to satisfy the requisite functionality.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
5/29/08

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135